BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan pesat jaringan internet telah membawa dampak signifikan dalam kehidupan masyarakat modern. Internet tidak hanya menjadi media komunikasi, tetapi juga menyediakan berbagai layanan seperti *web server, File Transfer Protocol (FTP), e-mail,* serta transaksi publik melalui e-commerce, e-*banking, e-government,* dan lainnya. Pemanfaatan internet telah meresap ke berbagai lapisan masyarakat, termasuk perusahaan, instansi pemerintahan, perkantoran, perumahan, universitas, dan sebagainya. Keberhasilan *internet* dalam memfasilitasi komunikasi dan *transfer* data menjadikannya bagian integral dari kehidupan sehari-hari.

Namun, seiring dengan manfaatnya, *internet* juga membawa risiko, terutama dalam hal keamanan jaringan. Perusahaan dan instansi yang terkoneksi dengan internet sering kali menjadi target gangguan dan serangan siber, yang dapat mengancam keberlanjutan informasi dan data yang dimiliki. Serangan seperti *Denial of Service (DoS) dan Distributed Denial of Service (DDoS)* menjadi ancaman utama karena mampu menghentikan layanan atau merusak ketersediaan data.

Serangan-serangan tersebut, termasuk *UDP flood, SYN flood,* dan *ICMP flood,* dapat menyebabkan gangguan serius pada sistem dan layanan jaringan. sebuah universitas di Indonesia dilaporkan mengalami serangan *DDoS* pada tahun 2023 yang mengakibatkan gangguan besar pada sistem pembelajaran daring dan administrasi kampus. Insiden ini dilaporkan oleh *Cyberthreat.id* yang mencatat peningkatan signifikan dalam frekuensi dan kompleksitas serangan *DDoS* di seluruh dunia. Demikian pula, berbagai instansi di sektor keuangan dan pemerintahan juga menjadi sasaran serangan tersebut, menyebabkan kerugian

finansial dan merusak reputasi.

Sekolah Menengah Kejuruan Negeri 3 Bengkalis sebagai lembaga pendidikan di Indonesia turut merasakan dampak perkembangan teknologi dan kebutuhan akan keamanan jaringan. Meskipun belum mengalami serangan besar, SMKN 3 Bengkalis tetap rentan terhadap potensi ancaman siber, terutama mengingat bahwa sistem keamanan yang diterapkan saat ini hanya mencakup aspek dasar seperti *gateway*. Kurangnya pemahaman dan kesadaran mengenai risiko serangan siber membuat lembaga ini perlu meningkatkan sistem keamanannya untuk melindungi data dan informasi yang dimiliki.

Salah satu solusi yang dianggap efektif untuk meningkatkan keamanan jaringan adalah dengan menggunakan fitur *firewall raw* pada *MikroTik RouterOS.* Fitur *firewall raw* adalah teknologi yang memungkinkan penyaringan paket data sebelum masuk ke proses *connection-tracking*, yang merupakan tahap di mana koneksi diidentifikasi dan dilacak. Dengan melewatkan proses ini, *firewall raw* dapat mengurangi beban *CPU* yang signifikan, terutama dalam menghadapi serangan *DoS/DDoS* yang mengirimkan volume besar paket tidak diinginkan. Menurut dokumentasi resmi *MikroTik* dan studi dari *MikroTik Academy*, pengurangan beban *CPU* ini dapat meningkatkan kinerja router secara keseluruhan, menjaga kestabilan jaringan, dan memungkinkan respon yang lebih cepat terhadap ancaman.

Selain efisiensi kinerja, *firewall raw* juga menawarkan fleksibilitas yang lebih besar dalam pengaturan aturan penyaringan paket. *Artikel* dari *Network Computing* (2022) menyebutkan bahwa *firewall raw* memungkinkan administrator jaringan untuk membuat aturan yang lebih spesifik dan terperinci, sesuai dengan kebutuhan keamanan yang unik dari suatu organisasi. Dengan demikian, *firewall raw* memberikan kontrol yang lebih mendalam dan responsif terhadap berbagai jenis ancaman.

Penelitian ini bertujuan untuk mengeksplorasi dan mengimplementasikan *fitur firewall raw* pada *MikroTik RouterOS* di SMKN 3 Bengkalis, dengan harapan dapat meningkatkan keamanan jaringan dan melindungi integritas data dari ancaman serangan siber.

1.2 Rumusan Masalah

Dari uraian Latar Belakang diatas, penulis dapat menyimpulkan beberapa rumusan masalah yaitu :

1 Bagaimana membanggun keamanan jaringan di SMKN 3 BENGKALIS ?

2 Bagaimana melakukan pengujian pada *router mikrotik* menggunakanserangan *Udp Flood, Syn Flood,* dan *Icmp Flood*?

3 Bagaimana mengatasi serangan *UDP Flood, SYN Flood*, dan *Icmp Flood* Menggunakan *firewall Raw* ?

1.3 Batasan Masalah

Untuk menghindari adanya penyimpangan maupun pelebaran pokok masalah dalam penyusunan penelitian ini maka di buat batasan masalah yaitu :

1. Metode pengamanan menggunakan *Firewall Raw* pada *Mikrotik.*
2. Skenario penyerangan menggunakan metode serangan *Udp Flood SynFlood*, dan *Icmp Flood* pada saat proses jaringan *Router* sedang beroperasi.
3. Penyerangan dilakukan menggunakan sistem operasi Kali Linux dan Loic.
4. Topologi Jaringan yang digunakan hanya sesuai dengan yang adadi SMKN 3 Bengkalis.

1.4 Tujuan

Adapun tujuan Tugas Akhir ini adalah :

1. Membangun sistem kemanan jaringan *router mikrotik.*
2. Melakukan penyerangan menggunakan metode *Udp Flood*, *Syn Flood, dan Icmp Flood Attack* terhadap *Router mikrotik*
3. Meningkatkan keamanan jaringan menggunakan *farewall raw* pada *Router board mikrotik*

1.5 Manfaat

Manfaat dari penelitian ini adalah :

1. Mengetahaui cara melakukan pengamanan terhadap *routerboard mikrotik*
2. Mengetahaui dampak serangan *Udp flood*, *Syn Flood,* dan *Icmp flood* pada

Routerboard Mirotik

3. Mengetahui bukti digital pada perangkat *router* yang telah di lakukan penyerangan